Using Artificial Intelligence (AI) To Help Keep Your Financial Data Safe

Ways Your Financial Data Can Become Compromised

Your financial data may not be as safe as you think.

Cybercrime is a growing threat to businesses of all sizes and includes:

- ✓ **Phishing,** where people log in and use their passwords to access websites that look real but are designed to capture the user's credentials
- ✓ **Weak or missing encryption,** which allows hackers to gain access to your data while being stored, transmitted or used
- ✓ **Misconfigured systems,** which allow cybercriminals access to your system
- ✓ **Malware such as ransomware,** where attackers lock down your data and require you to pay a ransom for its release
- ✓ **Employees using weak passwords,** or using them more than once, which hackers then discover and use

How Artificial Intelligence (AI) Can Help Protect Against Financial Data Threats

Artificial intelligence-focused security can supplement and enhance traditional cyber security systems and help you protect your customer's personal identifiable information (PII), such as by:

Identifying and responding to potential phishing emails by using algorithms to detect them and remove them from one's inbox

Being built into a security system's foundation to improve reliability and efficiency

Predicting possible threats to firewalls and monitoring. For example, AI can identify a user trying to access content that he or she is unauthorized to, limiting access until it's determined that the request is legitimate

Maintaining the encryption of data while it's being analyzed to help maintain security

Enabling security solutions to run 24/7 and responding to potential threats immediately

Identifying weaknesses in a cybersecurity system, such as issues with authentication, applications or users.

You can also help reduce the risk of financial data threat by having employees:

- Use an encrypted virtual private network (VPN) when working from home
- Maintain updated firewall and antivirus software on their laptops
- Maintain strong passwords and change them regularly
- Keep their computers password-protected and locked up when not in use

DFIN

DFINSOLUTIONS.COM

Sources: cloudtweaks.com/2020/04/keep-documents-secure-remote-work | workflowmax.com/blog/how-to-keep-your-data-safe-when-working-remotely | insureon.com/blog/what-you-need-to-know-about-remote-working-risks balbix.com/insights/attack-vectors-and-breach-methods | embroker.com/blog/types-of-cybercrimes